



2136
41

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of : **Confirmation No. 9406**
Hisashi INOUE et al. : Docket No. 2000_1451A
Serial No. 09/716,221 : Group Art Unit 2136
Filed November 21, 2000 : Examiner P. Parthasarathy

APPARATUS AND METHOD FOR EMBEDDING
INFORMATION FOR TAMPER DETECTION AND
DETECTING TAMPER AND RECORDING
MEDIUM HAVING PROGRAM FOR CARRYING
OUT THE METHOD RECORDED THEREON

THE COMMISSIONER IS AUTHORIZED
TO CHARGE ANY DEFICIENCY IN THE
FEE FOR THIS PAPER TO DEPOSIT
ACCOUNT NO. 23-0975.

SUPPLEMENTAL RESPONSE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RECEIVED

AUG 17 2004

Technology Center 2100

Sir:

Further to the Response filed August 6, 2004, please amend the above-identified application
as follows:

AMENDMENTS TO THE ABSTRACT

Kindly replace the original abstract (page 56) with the following substitute abstract.

ABSTRACT OF THE DISCLOSURE

~~An object of the present invention is to provide an information embedding/tamper detecting apparatus and method capable of distinguishing between changes caused by image processing and intentional image tampering, and further capable of localizing, on a regional basis, a tampered position on an image.~~

An object of the present invention is to provide an information embedding/tamper detecting apparatus and method capable of distinguishing between changes caused by image processing and intentional image tampering, and further capable of localizing, on a regional basis, a tampered position on an image. A tamper-detection-information embedding apparatus 1 divides the image into a plurality of frequency bands to obtain transform coefficients, and then generates a pseudo-random number series by using key data, and further generates authentication data. The key data and the authentication data are embedded in the transform coefficients of MRA and MRR, respectively. the image in which the information is embedded is reconstructed by using MRA and MRR. A tamper-detecting apparatus 2 extracts the key data from MRA obtained by dividing the image into frequency bands and generates the authentication data assumed to have been embedded, and further extracts the embedded information from MRR. The image is divided in to a plurality of blocks composed of a predetermined number of pixels. For each block, an information series embedded in the transform coefficients of MRR representing the same spatial region as the unit block is compared, for verification, with the corresponding authentication data series so that the tamper is determined on a regional basis.